Notice of Allowability	Application No.	Applicant(s)	
	09/727,904	JAKOBSSON ET AL.	
	Examiner	Art Unit	
	Bradley B. Bayat	3621	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *June 17, 2005*.

2. ☒ The allowed claim(s) is/are *1-17*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

DETAILED ACTION

This communication is in response to the decision rendered by the Board of Patent Appeals and Interferences issued on June 17, 2005.

- Claims 1-17 are allowed.
- Claims 18-20 are canceled.

EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

The Board of Patent Appeals and Interferences necessitated authorization for this examiner's amendment as per the decision issued on June 17, 2005.

The claims have been amended as follows:

1. (Previously presented) A method for controlling access to one or more information items purchasable from a merchant and accessible over a network, wherein a user interested in a given information item is permitted to access a corresponding signed ciphertext of the given information item, the signed ciphertext having at least a first ciphertext portion, the method comprising the steps of receiving from the user a blinded version of the first ciphertext portion of the signed ciphertext in conjunction with a request from the user for purchase of the given information item from the merchant; and decrypting the blinded version of the first ciphertext portion and returning to the user the resulting decrypted blinded version of the first ciphertext portion, wherein the resulting decrypted blinded version provides information that is utilized by the user in conjunction with accessing the given information item in a manner such that the

merchant is unable to identify the given information item purchased by the user.

2. (Previously presented) The method of claim 1 "wherein the signed ciphertext for the given information item comprises the first ciphertext portion, a second ciphertext portion, an unencrypted description of the information item, and a tag, with at least a portion of the tag comprising a signature.

3. (Previously presented) The method of claim 2 wherein the signature utilizes at least a part of the first ciphertext portion as a public key.

4. (Previously presented) The method of claim 1 wherein the first ciphertext portion comprises a symmetric key encrypted using a public key associated with the merchant.

5. (Previously presented) The method of claim 1 wherein the first ciphertext portion is encrypted using an ElGamal encryption technique.

6. (Previously presented) The method of claim 1 wherein the signed ciphertext is signed using a Schnorr signature.

7. (Previously presented) The method of claim 1 wherein the signed ciphertext further includes a second ciphertext portion corresponding to an encrypted version of the given information item.

8. (Previously presented) The method of claim 1 wherein the user verifies a signature of the signed ciphertext before requesting purchase of the given information item.

9. The method of claim 1 wherein the decrypting step is implemented in a payment server associated with the merchant.

10. (Previously presented) The method of claim 1 wherein the decrypted blinded version of the first ciphertext portion returned to the user further comprises a proof of correct decryption that allows the user to check that the decrypted blinded version for correctness.

11. (Previously presented) The method of claim 1 wherein the decrypted blinded version of the first ciphertext portion returned to the user comprises a blinded key that when unblinded by the user is used to decrypt a second ciphertext portion of the signed ciphertext so as to obtain the purchased information item.

12. (Previously presented) The method of claim 1 wherein the decrypting step is implemented in at least part of a set of multiple rounds, with the user providing a blinded ciphertext and receiving a corresponding decryption result for each of the rounds.

13. (Previously presented) The method of claim 12 wherein the decrypting step is implemented in j rounds, and wherein for each of the first j-1 of the rounds the user provides a blinded ciphertext and receives in response a corresponding decryption result that is subsequently reblinded by the user and provided as the blinded ciphertext for the next round, and wherein a

plaintext generated after the jth round provides the information that is utilized by the user in conjunction with accessing the given information item.

14. (Previously presented) The method of claim 12 wherein the decrypting step is implemented in part of a set of j rounds, and wherein for each of the first j-1 of the rounds the user provides a blinded ciphertext and receives in response a corresponding decryption result, and wherein a plaintext generated after one of the first j-1 rounds provides the information that is utilized by the user in conjunction with accessing the given information item.

15. (Previously presented) The method of claim 1 wherein the merchant establishes different public keys for use with different ones of a plurality of information items purchasable from the merchant.

16. (Previously presented) A processor-based system for controlling access to one or more information items purchasable from a merchant and accessible over a network, wherein a user interested in a given information item is permitted to access a signed ciphertext version of the given information item, the signed ciphertext version having at least a first ciphertext portion, and wherein the system is operative: (i) to receive from the user a blinded version of the first ciphertext portion of the signed ciphertext in conjunction with a request from the user for purchase of the given information item from the merchant; and (ii) to decrypt the blinded version of the first ciphertext portion and return to the user the resulting blinded version of the first ciphertext portion, wherein the resulting blinded version provides information that is utilized by

the user in conjunction with accessing the given information item in a manner such that the merchant is unable to identify the given information item purchased by the user.

17. (Previously presented) A machine-readable medium containing one or more software programs for controlling access to one or more information items purchasable from a merchant and accessible over a network, wherein a user interested in a given information item is permitted to access a corresponding signed ciphertext having at least a first ciphertext portion, and wherein the one or more programs when executed implement the steps of: receiving from the user a blinded version of the first ciphertext portion of the signed ciphertext in conjunction with a request from the user for purchase of the given information item from the merchant; and decrypting the blinded version of the first ciphertext portion and returning to the user the resulting blinded version of the first ciphertext portion, wherein the resulting blinded version provides information that is utilized by the user in conjunction with accessing the given information item in a manner such that the merchant is unable to identify the given information item purchased by the user.

18. (CANCELED.)

19. (CANCELED.)

20. (CANCELED.)

ALLOWABLE SUBJECT MATTER

Claims 1-17 are allowed over the prior art of record.

The following is an examiner's statement of reasons for allowance:

The closest prior art of record is U.S. Patent No. 5,754,656 to Nishioka et al. and U.S. Patent No. 6,275,936 to Kyojima et al.

As the rendering of the decision by the Board of Patent Appeals and Interferences on 17 June 2005 clearly states, the closest prior art of record Kyojima et al., do not disclose "a blinded version of a ciphertext portion of a signed ciphertext." Furthermore, as per the Board's decision, although Nishioka et al. refers to ciphers and signatures, sufficient motivation is lacking that would lead the artisan to make the proposed combination as claimed. Accordingly, as per the Board's decision, neither reference individually or in combination "specify the particular technique employing a blinded version of a first ciphertext portion of a signed ciphertext."

The relevant portion of the claims as indicated above recites: "receiving from the user a blinded version of the first ciphertext portion of the signed ciphertext in conjunction with a request from the user for purchase of the given information item from the merchant."

Method claims 2-15 are dependent upon claim 1; system claim 16 and machine-readable medium claim 17 have all the limitations of independent claims 1 and are allowable as indicated above.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

CONCLUSION

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Bradley B. Bayat whose telephone number is 571-272-6704. The examiner can normally be reached on Tuesday - Friday 8 a.m.-6:30 p.m. and by email: bradley.bayat@uspto.gov. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, James Trammell can be reached regarding urgent matters at 571-272-6712.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Any response to this action should be mailed to:

Commissioner of Patents and Trademarks
Washington, D.C. 20231

Or faxed to:

(571) 273-8300 - Official communications; including After Final responses.

(571) 273-6704 - Informal/Draft communications to the examiner.

JAMES P. TRAMMELL
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 3600

Bradley B. Bayat
Examiner
September 19, 2005